Anatomy, Dissection, and Mechanics of an Introductory Cyber-Security Course's Curriculum at the United States Naval Academy

Christopher Brown, Frederick Crabbe, Rita Doerr, Raymond Greenlaw*,
Chris Hoffmeister, Justin Monroe, Donald Needham, Andrew Phillips, Anthony Pollman,
Stephen Schall, John Schultz, Steven Simon, David Stahl, Sarah Standard

United States Naval Academy
Annapolis, Maryland 21402
United States of America

ABSTRACT

Due to the high priority of cyber-security education, the United States Naval Academy rapidly developed and implemented a new cyber-security course that is required for all of its first-year students. During the fall semester in 2011, half of the incoming class (about 600 students) took the course through a total of 31 sections offered by 16 instructors from a variety of disciplines and backgrounds. In the following spring semester, the remaining half of the first-year students will take the course. This paper explains the motivation that instigated and drove course development, the curriculum, teaching mechanics implemented, personnel required, as well as challenges and lessons learned from the first offering of the course. The information contained in this paper will be useful to those thinking of implementing a technical course required of all students at the same level in an institution (in our case first-year students) and particularly those interested in implementing such a course in cyber security.

Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education – *curriculum, information systems education, computer science education, literacy, self-assessment*

General Terms

Documentation, Security

Keywords

Active Learning, Computer Security Awareness, Cyber-Security Education, Cyberspace Policy Review, Freshmen Required, Information Assurance, Naval Academy, Networks

*Contact author phone and email: +1-410-293-6806, greenlaw@usna.edu.

ITiCSE'12, July 3–5, 2012, Haifa, Israel.
Copyright 2012 ACM 978-1-4503-1246-2/12/07...$10.00.

1. INTRODUCTION

In May 2009, President Obama's Cyberspace Policy Review included an action item to "expand and train the workforce, including cyber security expertise in the Federal government" [7]. In response to this charge, the United States Naval Academy's (USNA's) Academic Dean & Provost created a Cyber Warfare Ad Hoc Committee. This committee consisted of faculty and staff members with broad representation from across the campus. Their charge was to explore and define the scope of understanding of cyber security needed by Midshipmen (undergraduate students at USNA), as future naval officers. The committee consulted with the Office of the Chief of Naval Operations and Commandant of the Marine Corps staffs, and sought their input and perspectives on the education USNA's graduates should receive to help address the needs of the Navy and Marine Corps. The committee also analyzed the other service academies' inclusion of cyber-warfare concepts in their curricula, and examined graduate-level programs to determine the foundational education and skills necessary for entry into their cyber-warfare-related curricula.

In August 2009, USNA's Cyber Warfare Ad Hoc Committee delivered its Initial Report that included a recommendation to create a required core course providing a technical foundation for undergraduate cyber-warfare education for all students regardless of academic major [6]. The unanimous view of the committee was that the course be technically oriented, focused on naval applications and case studies, and delivered in a hands-on, lab-based format. This course was intended to form the technical basis for continued cyber-security education that could be expanded upon as appropriate within the various majors. In the spring semesters 2010 and 2011, a prototype course based on the Cyber Warfare Ad Hoc Committee's recommendations was developed, delivered, and refined by USNA's Computer Science Department.

In April 2010, USNA's Academic Dean & Provost formed an Ad Hoc Committee on Cyber-Security Curriculum Options. This committee, comprised of three senior professors from the Divisions of Engineering & Weapons, Humanities & Social Sciences, and Mathematics & Sciences, was charged with examining a variety of approaches for integrating cyber concepts in the core curriculum. Ultimately, the committee recommended a two-course, technically-oriented sequence: the first to be taken by all students during their initial year and the second, providing more technical depth, to be taken by all students during their third

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JUL 2012**	2. REPORT TYPE	3. DATES COVERED **00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE
Anatomy, Dissection, And Mechanics Of An Introductory Cyber-Security Course?s Curriculum At The United States Naval Academy

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
United States Naval Academy,Annapolis,MD,21402

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Prepint, ITiCSE2012 - ACM SIGCSE Conference on Innovation and Technology in Computer Science Education, July 1-5, Haifa, Israel

14. ABSTRACT

Due to the high priority of cyber-security education, the United States Naval Academy rapidly developed and implemented a new cyber-security course that is required for all of its first-year students. During the fall semester in 2011, half of the incoming class (about 600 students) took the course through a total of 31 sections offered by 16 instructors from a variety of disciplines and backgrounds. In the following spring semester, the remaining half of the first-year students will take the course. This paper explains the motivation that instigated and drove course development, the curriculum, teaching mechanics implemented personnel required, as well as challenges and lessons learned from the first offering of the course. The information contained in this paper will be useful to those thinking of implementing a technical course required of all students at the same level in an institution (in our case first-year students) and particularly those interested in implementing such a course in cyber security.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

year. This paper focuses on the development of the first in that sequence of two cyber core courses. And while the term "cyber" is currently used in many ways, for the purposes of this paper, we use it to refer to the totality of the space in which new kinds of computer crime, terrorism, espionage, and warfare are taking place.

Although USNA settled on one course in the first year and a second course in the third year, numerous other options were considered. No other option was deemed as easy to implement; in fact, at the time the options were formally presented (February 2011), the general consensus of the Committee, and all others who had been involved, was that the earliest possible implementation date for any option selected would be August 2012. In February 2011, the Committee's recommendation was approved, but the implementation date was to be August 2011—a mere six months later. There were many roadblocks to overcome to meet this deadline, some that would be typical of any academic campus (such as faculty-led, curriculum-review processes and faculty-senate votes and recommendations). In this instance the ground rules usually applied at USNA were modified given the short deadline and the importance of the initiative. USNA leadership made two things clear from the outset: the implementation deadline of August 2011 was immovable, and the inclusion of the new cyber course as a first-year, lab-oriented, technical-core course was non-negotiable. Other than that, all other specific details from course content to faculty development to assessment measures were left up to the faculty to debate and decide. So, in that context and with only six months to act, all faculty approval processes were conducted in parallel with course development and implementation planning.

There were many other significant challenges as well, ranging from determining what technical content to teach, to who would teach the course and how USNA would identify and prepare those faculty members within a six-month time frame. Perhaps the greatest challenge of all was how to teach this technical course to a new class of 1,200 first-year students (600 each semester) in a way that did not simply add more work to an already very busy schedule for the first-year students. The phrase "very busy" is used because students at the service academies have many demanding military obligations that are not common at other institutions and classroom attendance is required. At USNA, all first-year students take the same "core" of courses in their first year, an academic workload that amounts to 11 courses consisting of 35 credits over two semesters. To make room for the new cyber-security course, one of the existing core courses was moved to the second year (which itself resulted in additional curriculum changes and shifts) thereby resulting in only a single hour increase in course time. While finding the "slot" in the first-year schedule was challenging, a greater challenge was how to teach another technical subject (in addition to the required science-and-engineering-focused calculus and chemistry core courses) in such a way that the students would be engaged in the material sufficiently so that the difficulty associated with the technical nature of the content would be compensated for by the motivation of learning about the practical aspects of both offensive and defensive cyber security. The mantra was "Make it Navy relevant and make it exciting!" That outcome was considered essential; in a technical course involving two lecture hours and two lab hours per week, the end result needed to be that the students really enjoyed and learned the content, and that their day-to-day behavior regarding the use of social media, the Internet, wired and wireless networks, and so on, would now be much-better informed and positively affected by their new understanding of the risks and threats associated with cyber security.

Teaching cyber security to computer science and related majors is not a particularly new idea; many higher-education institutions offer courses in computer/network security, and a few even offer full degree programs in cyber security. Finding undergraduate, graduate, and even certification courses in cyber security is not especially challenging. However, the Naval Academy was in search of a stand-alone, technical, hands-on course with a broad range of cyber-security content that could be taught to every first-year student, regardless of their intended major or computer knowledge/skills, and further which served to significantly enhance the student's awareness and understanding of the risks and threats associated with cyber security, especially those that are relevant to the U.S. Navy and Marine Corps.

Before launching our first-year, cyber-security course, we contacted the two other major military service academies to determine what cyber-security education was provided to their students. The United States Air Force Academy (USAFA) requires an introductory computer-systems and information-technology course that includes five lessons focused on the fundamentals of computer security. In the summer of 2011, USAFA rolled out an elective two-week, full-time program to about 90 cadets that provides them with a hands-on experience in cyber security [Gibson, personal communication, 2011]. The content of the elective course has perhaps a 40% overlap with the content of the USNA first-year course. Similarly, the United States Military Academy's curriculum includes an information-technology-related course, but the focus is not in computer or network security [1].

2. COURSE CONTENT

The Cyber Warfare Ad Hoc Committee's Initial Report describes Cyber Warfare as "...a technical academic core of tightly inter-related subject matter, as well as a wide range of important topics that, while dependent on the technical core for fullest appreciation, are not dependent on each other. Stated another way, cyber warfare is comprised of, first, a foundational component, dealing with a set of interconnected fundamental technical concepts, and second, a wide range of interdisciplinary topics, touching upon the areas of law, political science, strategy and tactics, policy, ethics, and the study of foreign languages and culture" [6]. The Initial Report recommended creating a required core course that covered the technical foundations of Cyber Warfare; a course that is technical in nature, relevant to naval officers, and delivered in a hands-on and engaging manner.

The required cyber-security course now offered at the Naval Academy meets the required recommended in the Initial Report. The fundamental goals for the course are that students acquire:

• an understanding of the basic physical and virtual architecture of cyberspace, including: the individual computer and program, the physical components and protocols of a network and the Internet, and the distributed client-server system that is the world wide web,

• hands-on experience with basic components of the physical and virtual architecture of cyberspace and the ability to relate that experience to the larger system,

• an understanding of the Department of Defense's pillars of Information Assurance (availability, integrity, authentication, confidentiality, and non-repudiation), the inherent vulnerabilities of information systems that endanger these properties, defensive measures to ensure that information systems retain these properties, and offensive measures that can be used to violate these pillars, and

- hands-on experience with some basic defensive and offensive practices in cyberspace, and the ability to relate that experience to new or more sophisticated attacks and defenses.

2.1 Hands-On Aspects

The hands-on element of the course is crucial to delivering a meaningful academic, technical, and engaging experience. It provides students with concrete experiences that they can relate to new or more-complex situations and/or technologies they encounter in order to make sense of them. For example, the lessons devoted to programs look at only simple programs, but as a hands-on exercise, the students are asked to provide unexpected input that crashes these programs or that make them behave in unintended ways. The lessons ask students to modify these simple programs to deal gracefully with bad input so that they get concrete hands-on experience with "patching" these kinds of coding errors, and thus see firsthand how hard it is to anticipate all the ways that input might be problematic. For example, the students edit the programs to escape certain characters and they edit conditional statements. The bad-input concept recurs in the section on attacks against network services. A network service is simply a program that sits and waits for input from a network connection rather than a keyboard or mouse. If an attacker can send that program input that the programmer did not anticipate and deal with gracefully, the service can be made to crash or do unintended things. Through careful design, almost every class meeting involves hands-on activities. The activities provide students with concrete experiences from which to reason and generalize, and a strong foundation for critical thinking and problem solving.

2.2 Course Components and Premises

The cyber-security course is divided into three sections: the Cyber Battlefield, Models and Tools, and Cyber Operations. One cannot begin to instruct students in cyber attack and cyber defense until students actually understand the space in which these actions take place, so the first part of the course introduces students to the "Cyber Battlefield": digital data, computer hardware, operating systems, programs, the web, networks, wireless networks, and the Internet. By covering these elements of cyberspace, students get hands-on experience with them and also see a variety of "bad things" that can happen (for example, clicking on a hyperlink to some innocuous site but instead being sent somewhere else, crashing programs with bad input, injecting malicious code into a website to crash it, stealing user names and passwords with malicious e-mail attachments, and so on). The students not only see how systems are supposed to work, but also understand how malicious actions break them.

The second section of the course is "Models and Tools." In this section students learn formal models of "security" and "risk" for information systems. To make concrete and compelling what could be abstract and lacking motivation, these models are related back to the "bad stuff" that the students saw happening in the first part of the course. For example, we show how an injection attack that redirects one website to some other site is an attack on *availability*. The models are then used to understand and reason in a principled way about new situations. With this new-found understanding of what security really means for an information system (that is, what things we are really trying to protect) we look at some of the fundamental tools used to provide security: firewalls, symmetric encryption, cryptographic hashing, authentication, asymmetric encryption, and digital certificates.

Finally, once the students understand the battlefield, what they are trying to defend (or attack), and what defenses they can employ (or must defeat), we move to the third and final part of the course: "Cyber Operations." In this section of the course, we look at cyber reconnaissance, attack (including malware), defense, forensics, and case studies. The course culminates in a series of three hands-on labs in which each section of students is divided into two teams, with each team responsible for their own network. They reconnoiter their opponent's network, attack their opponent's network, and finally defend (that is, harden) their own network and re-attack their opponent's hardened network. These activities occur on virtual hosts and networks served from a system that is (students access the virtual sandbox environment via the VMware *Vsphere*™):
a) completely isolated from the Naval Academy's public network,
b) able to be reset in seconds to its initial configuration following each lab period, and
c) indistinguishable from a real physical network.

3. COURSE MECHANICS

In this section we discuss the "mechanics" involved in teaching the first-year, cyber-security course: the assumed background of the incoming students; the lecture and lab delivery; homework and exams; student perspective, student and instructor communication mechanisms during the semester; and the means by which additional tutoring and review were available.

3.1 Student Background

Realizing that the cyber-security course was required for each student entering their first year at USNA, it was anticipated that there would be a wide variety of backgrounds encountered with first-year students. USNA is a highly selective institution. In the class of 2015, there are 993 men and 236 women, or roughly 19% female [8]. The students come from all 50 states, U.S. territories, and several foreign countries. Over 50% of the class of 2015 ranked in the top 10% of their high school class, and 50% of the students scored from 590–720 (out of 800) on the SAT Verbal and 50% scored from 610–730 on the SAT Math [8]. We assumed that each first-year student had some (though not much) computer experience along with a basic understanding of the Windows™ operating system and its associated applications. But, given the first-year nature of this course, there could be no prerequisites.

3.2 Course Delivery

As noted earlier, instructors taught material through both lecture and lab format. Online student lecture or lab notes, as appropriate, were available for each of the 41 lessons. Both internal (available only on campus) and external (http://www.usna.edu/cs/si110/) websites were created. The course policies, support materials, and supplemental resources were also available on both websites. The internal website contained links to all software resources needed for the course;

however, not all these resources were available on the external site. The external site existed so that students could access course material when travelling for an athletic or extra-curricular event. Additionally, there was a website accessible only to instructors to provide lesson plans, laboratory guides, and homework solutions. All of the lectures included a link to a homework assignment that was due the next class period. Every instructor also utilized an in-class, individual message board for sharing links and demonstrating some web-based activities.

Following customary procedure at USNA, there were three exams administered for the course. In order to standardize exam grading across sections, a rubric was provided in order to determine the amount of partial credit to be awarded for wrong answers.

3.3 Student Perspective

We administered two in-class surveys at six and sixteen weeks as well as a course evaluation to all students in order to gauge whether the course objectives were met and the students improved computer security knowledge and awareness. Roughly 94% of the students felt that the hands-on activities were helpful. About two-thirds of the students indicated that they truly enjoyed the hands-on activities, while about 95% of the remaining third indicated that they enjoyed the hands-on activities somewhat. Roughly 27% of the students felt they lacked some of the requisite computer knowledge/skills at the start of the course, but of those just 13% felt that this deficiency was a problem. About 95% of the students said that they became more aware of the threats facing their computer than before they started the course, while about 4% indicated they were already highly aware of the existing threats. For each of the three main parts of the course (as described in section 2.1), between 88–95% of the students indicated that they either had a much-better or somewhat-better understanding of the key issues involved. In other words, as self reported, the course learning objectives were met by about 90% of the students.

3.4 Communication

Offering a new, required cyber-security course to first-year students with a newly-indoctrinated set of instructors, some who did not have a computer-science background and/or had never taught at USNA before, meant that communication (constant, consistent, and concise) was paramount. An email alias was created for each of the 31 course sections which were further grouped into an overall course email alias. Instructors regularly used their section's email alias for specific class updates, while the course coordinator was the primary user of the overall course alias for more-global course announcements. An instructor-email alias (consisting of the 16 course instructors) was also created and used for a wide variety of purposes.

While instructors maintained almost daily email contact, mandatory weekly instructor meetings were held to review the previous week's classes, as well as to prepare for the upcoming week's material. These meetings were also used to gauge the overall progress of the students, as well as to discuss any content issues for the course. Typical examples of content issues were discussions about the arrival of new hardware/software or how a lecture/lab could be better presented next semester. When a particularly involved lab was forthcoming, the weekly instructor meetings were devoted to stepping through the lab.

3.5 Additional Instruction

Since this cyber-security course had never been taught at USNA before, a support structure for student learning was critical. The offering of any required college-level course comes with it the responsibility of providing tutoring, additional review, and outside of class extra instruction. USNA's cyber-security course offered all three. Using the model of other USNA technical core courses, an evening, group-study program was instituted. This Midshipmen Group Study Program (MGSP) was available Sunday–Thursday evenings, led by junior- and senior-year computer science and information technology majors selected by USNA's Center for Academic Excellence and the Computer Science Department. MGSP was augmented with special review sessions for each of the 6-week, 12-week, and final exams. These well-attended sessions, held during the MGSP timeframe on a Sunday evening prior to the exam, reviewed key learning objectives and homework exercises while also answering student questions. For these reviews, numerous instructors and rooms were used. Some instructors supplemented exam reviews by offering evening online instruction using an online-meeting tool. Lastly, if more one-on-one tutoring was needed, students were encouraged to contact their instructor for additional help.

4. PERSONNEL REQUIRED

In order to successfully deliver this course, USNA needed to coordinate the efforts of personnel in diverse roles, from instructors, content developers, facility and technical support, to administrators.

4.1 Course Instructors

Having only six months lead time between the decision to deliver the cyber-security course and the start of the fall 2011 semester, there was considerable concern about where to find qualified instructors; hiring enough new faculty members (either part-time or full-time) with appropriate qualifications to teach cyber security is a very difficult proposition due to the high demand for this skill set. So, interested faculty members were sought from other departments, from the campus IT staff, and also from outside of the USNA academic community. As a result of these vigorous efforts, a diverse group of sixteen instructors taught the first semester. The faculty members assembled possessed various levels of technical expertise in cyber security. Some faculty members were active military officers who brought a great deal of relevant operational exposure gained during their previous career assignments. We should note that roughly 50% of the faculty members at USNA are military members who hold at least a Masters degree, and those percentages are the same for the Computer Science Department (CSD). Other instructors had a strong personal technical interest in the subject matter, while some had significant but non-technical experience.

4.2 Course Coordinator and Content Developers

Due to the technical nature of the course and the short timeline for implementation, several faculty members from the CSD were tasked with forming a course-coordination cadre to flesh out the course details fully. This group had four leaders. One developed much of the overall curriculum for the course, another led the hardware and software acquisition efforts and assisted with curriculum development, a third developed much of the lab-focused portions of the course, and a fourth formatted homework and solutions. The course content was developed mostly by the course coordinator, the instructors who taught the prototype of the course, and a small subset of the instructors. The development efforts began in earnest in April 2011 and continued full time throughout the summer and into the fall semester concurrent with the running of the cyber-security course. All courses at USNA have a course coordinator, so we did not need to create an entirely new model for developing and teaching this course. The benefits of a good course coordinator are that less-experienced instructors have a framework from which to deliver a strong class, and the efforts of one are leveraged so that faculty members do not need to duplicate work.

4.3 Facilities Manager

We designated an experienced faculty member as the course Facilitates Manager. This faculty member, who also taught the course, served as the main coordinator for hardware and software identification, acquisition and testing. We found that this approach worked well since it allowed the Course Coordinator to focus more fully on the task of developing course content. There were times when technical staff needed to drop everything they were doing to aid the facilities manager in addressing emergent problems with course hardware and software. Our facilities manager had the positional authority to expect immediate assistance from the technical support staff when required. Issues that prevented instructors from teaching the course effectively or prevented students from working on class material were given the highest possible priority, and the facilities manager and technical-support personnel did a good job in fixing any problems that developed unexpectedly.

4.4 Technical-Support Staff

This course required dedicated technical support. It was important to have technical-support staff available and ready to go to lab rooms to assist instructors with real-time issues. Although as we noted earlier, instructors practiced the labs during weekly instructor meetings, there were occasions when unexpected problems arose during labs. If instructors were not able to solve such problems themselves, they needed assistance from the technical-support staff, facilities manager, or course coordinator. Running such a course for the first time would be impossible with just faculty members supporting the course, as there are many network issues that need to be addressed. Our technical-support staff for the course included a contractor who had a high level of proficiency with computer security. Additionally, several staff members from the Academy's information technology staff were assigned to assist with the hardware and software support for the course.

4.5 Administrators

From the Superintendent to the Academic Dean & Provost to the Math & Science Division Director to the CSD Chair, administrators played a vital role in the successful rollout of the cyber-security course. (Note that at USNA the Academic Dean & Provost position is equivalent to the Vice President for Academic Affairs, and a Division Director is equivalent to a college level Dean.) They had to have vision; they had to instill the belief that this project could and would be implemented; they had to encourage faculty and set milestones; they had to provide resources and strong support for all personnel involved. And, most importantly, they had to remain flexible and keep expectations realistic. Our administration formed the appropriate committees, sought appropriate input for the course, listened to the feedback that they received, and helped guide the course through appropriate USNA approval channels. The administrators acted quickly in terms of hiring instructors and replacing lost technical staff. They helped as much as possible in expediting hardware and software requests which often can be notoriously slow in large organizations. And, they found creative ways to free up instructors to teach the course. The course received a great deal of media attention [2–5], and administrators worked on promoting the course both internally and externally. Without such a strong and dedicated administrative team, the course could never have been implemented. The challenge would simply have been too great for a department to take on alone.

5. LESSONS LEARNED AND RECOMMENDATIONS

Since many of the instructors were new to the course material, possessed varying levels of technical exposure to cyber security, and in some cases had never before taught at an undergraduate institution, USNA offered a two-week summer preparatory "boot camp" in August 2011. During this session, the entire course was presented and beta tested. The "boot camp" gave the instructors the opportunity to familiarize themselves with the content and provided the course coordinators the feedback necessary to refine material and test the support equipment. Fortunately, all instructors taught for the full semester without any emergency departures. Nevertheless, one recommendation is to train and maintain a list of possible replacement instructors in the event of an unexpected departure.

Section 3.4 discussed the weekly instructor forum, which was conducted in one of the student classrooms for faculty to review successes, challenges, and upcoming content. These meetings, together with the instructor-email alias, provided additional opportunities to test and improve upcoming labs and lectures. The instructor alias facilitated an ongoing exchange of ideas and a venue for capturing experiences and challenges encountered during the course. All email aliases that were established were keys to communicating successfully and efficiently.

As discussed in section 3.2, the primary reference for students was the course website, which was a very successful tool for students and instructors. The technical orientation and dynamic nature of the course necessitated the robustness and currency of the website, as it was the primary source of lesson material for the students. A secondary source of information was the required course textbook; however, most students never used their textbook for this course, and therefore the textbook requirement needs to be reassessed. The student notes posted by the course coordinator were extensive and students read those more than the textbook.

The previously discussed student-learning support structure with MGSP, exam reviews, and extra instruction were extremely popular among the students, and their student opinion forms highlighted that fact. As expected, the sessions dedicated to exam review were the best attended with about 50% of students attending. For MGSP sessions, typically 10–20% of the students attended. USNA will soon offer evening cyber-security tutors in its Center for Academic Excellence, and this service is seen as a necessity for the course. Additionally, an “extra-help” non-credit class is being offered starting with the spring 2012 course. This “extra help” period is available to students that anticipate needing additional assistance and study time for most of the first- and second-year technical core courses at USNA.

A key miscalculation when developing the content for this course was the expectation that students would have a much greater level of basic computer skills at the start of the course. The reality was that while students were adept end users of computer technology, they superficially understood the concepts and practical applications of computer technology and basic user security. As a result of this realization, future iterations of this cyber-security course must be adapted to take the lack of basic skills into account. All first-year students are issued laptops at USNA and are required to use those machines extensively in the fall. For this reason we expect the 600 students taking the course during the spring will not be burdened by a similar lack of basic computing skills; they will have been using the machines for four months.

While the cyber-security course was technically oriented and hands-on, it unintentionally lacked sufficient real-world contextual reinforcement of the technical concepts discussed in the classroom. USNA’s Center for Cyber-Security Studies sponsors seminars and a lecture series with top-level, subject-matter experts discussing cutting-edge, cyber-security topics. And although these sessions were available to the student body at large and well attended, the incorporation of these events into the classroom would have provided one avenue for the needed contextual reinforcement. Additional contextual material should be integrated directly into course material. Since the required course textbook was insufficient at providing up-to-date content, online cyber-security articles may hold the key to deliver current and relevant supplemental and pre-read material.

The weekly utilization of hands-on laboratory exercises were instrumental in creating knowledge transfer and widely enjoyed by the majority of students, as indicated in course-wide evaluations. One downside to the exercises was the lack of laboratory assistants. Frequently, during the labs, the exercise was interrupted with competing individual technical issues or student questions. While the lab objectives were usually met, having (dedicated) assistance during the lab would have facilitated more-effective knowledge transfer for the class as a whole while providing the ability to address individual concerns.

Clearly, not all institutions can or would necessarily devote this amount of energy and resources to introducing an institution-wide course in cyber security. However we encourage other institutions to take some steps toward preparing students to handle emerging cyber-security threats. These steps might be any one of the following: the introduction of a non-technical, elective, cyber-security course that has no prerequisites, the introduction of a technical cyber-security course in a specific department such as information technology or computer science, the introduction of a short course on cyber security, or perhaps the incorporation of more cyber-security material into existing courses.

6. SUMMARY

By all measures the cyber-security course was successful. The course was implemented and provided to nearly 600 students in the fall semester with only six months notice. Overall, the learning objectives of the course as designed were met. The course was technically oriented with hands-on activities designed to reinforce the learning objectives. Although most of these students will not make their careers in cyber security, they will graduate with a better understanding of its fundamentals. Throughout this work we have highlighted many of the difficult challenges that were overcome to make the course a success. Finding qualified staff to teach/develop such courses and allocating the necessary resources are possibly the greatest challenges that an institution intending to design and implement a new curriculum will face. We did not observe meaningful differences in student outcomes attributable to a diverse set of instructors.

7. REFERENCES

[1] Academic Program. Curriculum and Course Descriptions. Office of the Dean. United States Military Academy. West Point, New York. DOI = http://www.dean.usma.edu/sebpublic/curriccat/static/index.htm.

[2] Brown, M. H. 2011. Naval Academy Preparing Officers for Cyberwarfare. Baltimore Sun. DOI = http://www.baltimoresun.com/news/maryland/education/bs-md-naval-academy-cyber-security-20111019,0,2371754.story.

[3] Carroll, C. 2011. Cyberwarfare Joins the Curriculum at Service Academies. Stars and Stripes. DOI = http://www.stripes.com/news/cyberwarfare-joins-the-curriculum-at-service-academies-1.158642.

[4] Witte, B. 2010. Military Academies Teach More Cyberwarfare. Navy Times. DOI = http://www.navytimes.com/news/2010/03/ap_cyberwarfare_030810/.

[5] Naval Academy Weaves Cybersecurity into Curriculum. DOI = http://defensesystems.com/articles/2011/03/08/naval-academy-adds-cybersecurity-courses.aspx.

[6] Needham, D., and Patrick, V. Initial Report of the Dean’s Cyber Warfare Ad Hoc Committee, USNA-CS-TR-2011-02. U.S. Naval Academy Computer Science Department, Annapolis, MD, 2011.

[7] President’s Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 2009. DOI = http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[8] United States Naval Academy. Class of 2015 Profile. DOI = http://www.usna.edu/admissions/USNA%202015%20Class%20Portrait.pdf